THE USE OF ENCRYPTION IN IT CONTROL AND IN THE SECURITY OF DATA AND INFORMATION

Tommie W. Singleton, School of Business, University of Alabama at Birmingham, Birmingham, AL 35294, (205) 934-8820, tsinglet@uab.edu,
Julio C. Rivera, School of Business, University of Alabama at Birmingham, Birmingham, AL 35294, (205) 934-8820. jrivera@uab.edu,
William A. Hailey, School of Business, University of Alabama at Birmingham, Birmingham, AL 35294. (205) 934-8820, whailey@uab.edu,
Edward M. Curry, School of Business, University of Alabama at Birmingham, Birmingham, AL 35294, (205) 934-8890, tops@uab.edu

ABSTRACT

This paper presents an overview of data encryption methods that may be used to protect data from unauthorized access. Data encryption has come to the forefront as an important method of protecting data due to legislation such as HIPAA as well as privacy concerns expressed by individuals. The authors examine the use of encryption in different situations by interviewing people in positions responsible for using or safeguarding data, as well as examining the literature regarding the application of encryption methods to business situations. This paper concludes by outlining the areas in which data encryption may be useful in safeguarding data.

INTRODUCTION

Much has been written and said about cyber-terrorism, identity theft, and the invasion of privacy in current news reports and articles, and certainly these problems pose serious threats to our society and to our security. According to a recent poll by The Information Technology Association of America, 75% of the individuals surveyed stated that they feared having their personal information misused. Also according to government and privacy advocacy groups, 700,000 cases of identity theft were reported last year, and in 2001, the credit card industry sustained billions of dollars in losses due to credit card fraud. [1]

The aforementioned crimes and issues have motivated Congress to pass two regulations which provide standards for the protection of consumer information. One regulation is the Health Insurance Portability and Accountability Act (HIPAA) which set standards for the security of medical records and pertinent identifiable individual health information. The other regulation is the Gramm- Leach- Bliley Act (GLBA, Public Law 106-102) which places requirements on financial institutions for the security and privacy of individual consumer financial information. The HIPAA regulation imposes civil and criminal penalties for "non-compliance due to willful neglect" (that is, fines of up to $50,000 per violation and one-year in prison). Congress is also considering The Financial Institution Privacy Protection Act which would strengthen The GLBA and mandate that directors and company officers be liable for up to $10,000 for each privacy violation. [1]

If laws and regulations "interpret protecting privacy", then protecting data, records, and information must involve using effective and secure encryption technology. For example, a 128-bit key-length encryption provides 2^88 times as many combinations as a 40-bit key-length encryption. In 1997, a 40-bit SSL encryption session was deciphered in about four hours by a college student who used the "brute - force "form of attack. It is estimated that using the same method of attack against a 128-bit SSL encryption session would take this same hacker more than a trillion years to effect decryption.[2]

The Advanced Encryption Standard (AES) which uses the Rijndael algorithm, the winner of a three-year competition involving the world's leading cryptographers, and which was developed to provide protection for sensitive government information well into the 21st century, uses block cipher encryption and long keys of 128-, 192-, and 256-bit lengths. Reportedly, it would take an advanced brute-force computer, which computes 90 billion keys per second, a million years to decipher a 112-bit AES key encryption and more than a thousand times longer to decipher a 128-bit AES key encryption.[3]

OVERVIEW OF ENCRYPTION AND ITS USES IN IT CONTROL AND SECURITY

Encryption is the process whereby data (and information) is encoded by using mathematical functions and algorithms so that it can not be read by anyone who does not know the passkey or password that decodes it. In terms of data security, encryption can function actively at the application level, the network level, and at the host level of data transmission and information flow.

The objective of encryption is to make data extremely unintelligible to unauthorized readers and astronomically difficult to decipher for the intruder or hacker. In this regard, encryption is dependent upon the use of random encryption keys (the randomness of the keys makes the encrypted data that much more difficult to attack). Not only are keys used to encrypt data, but they are also used to execute the decryption of data.

Not all encryption is alike and the security of encrypted data is dependent not only on the key size but also on the quality of the encryption technology and on the algorithm that is implemented in the encryption process. [4]

There are three general categories or approaches to the use of encryption: 1.Symmetric Key Encryption. 2. Asymmetric Key Encryption. 3. One-Way (Hash) Encryption.

Symmetric Key Encryption

In symmetric key encryption (also known as Private –Key Encryption) each user of the encryption system must have a copy of the single key that is used for both encryption and decryption. In symmetric key encryption there are two types of symmetric ciphers: block ciphers and stream ciphers. Although stream ciphers are twice as fast as block ciphers they require the use of unique keys whereas block ciphers permit the keys to be re-used. Some form of symmetric key block cipher technology is used in most DBMS's. A disadvantage of symmetric key encryption is that when it is set up or changed, a copy of the key must be

delivered by a secure means to the users of the system, and the key cannot be used to deliver the key to someone who does not have it. Also if the old key has been compromised, a key cannot be used to deliver a new one. [1]

In symmetric key encryption, the recommended key length is 128-bits or longer. With regard to data security, key length is of paramount importance because there are two ways to attempt to decipher symmetric key encrypted data: 1. The "guess and check" assault and 2. The "brute-force" method.

The "guess and check" assault is successfully executed when an algorithm that has been implemented in the encryption process is based on bad random number generation or is incorrectly implemented. The hacker guesses at a key and then he or she tries the key on a sample of the program's data. [3]

The "brute –force" method is implemented when a very powerful computer makes it feasible to create and test a number of keys in a very short period of time. For example, it has been reported that DES ciphers using 56-bit keys have succumbed to brute –force assaults in less than 24 hours (AES to the contrary uses long keys of 128-, 192-, and 256- bit lengths). [3]

If data is going to be encrypted for storage, symmetric key encryption is most commonly used. [3]

Asymmetric Key Encryption

Asymmetric Key Encryption (also known as Public Key Encryption) provides each user of the encryption system with a pair of keys: a public key and a private key. The key pairs are produced by using mathematical algorithms that permit any data encrypted by one key to be decrypted only by the other. Asymmetric key encryption is most frequently used to protect data during transmission and, as stated, it maintains one key as public and the other as private. A user sends copies of his or her public key to anyone who wants or needs it (however the private key is kept secret by the user) to send an encrypted message to the user. A message encrypted with the user's public key can only be decrypted with the user's private key. A message encrypted with the user's private key can only be decrypted with the user's public key. Therefore each user in a dialog must send its public key to the other user. [1]

The algorithms used in asymmetric key encryption make up the basis for "public key infrastructure" or PKI. PKI is based on a hierarchy of digital certificates that contain a user's public key and is certified or "signed" that the holder of one key of a pair of keys can trust any data that key decrypts as having been encrypted by the matching key. PKI also refers to a trust hierarchy based on public key certificates, and in other settings or applications, digital signature services that are provided to end users. The algorithms used for digital signatures are the RSA algorithm, the U.S.Government's Digital Signature Algorithm (DSA), and the elliptic curve algorithms. [1]

Asymmetric algorithms are mainly used for authentication and digital signature functions rather than for encrypting data. They are considerably slower than symmetric key algorithms which

make them not suitable for database encryption because they could adversely impact database performance. [4]

One-Way (Hash) Encryption

The algorithms used to hash data do not execute encryption on the data, but provide a one-way transformation of the data which may then be used to securely store the data or to verify its integrity. When a block of data undergoes "hashing" a "hash value" or unique digest of the data is produced that is of a fixed byte length. If new data arrives that should match the original, the new data is hashed and the two "hash values" are compared. The two values should be identical, if the data has not been altered or corrupted. If the data has been altered, the hash values will be different. [5]

One-way encryption is used for password data storage and authentication. In a network system, a user enters a password in the client software which hash encrypts the data and then sends it to the Network Operating System (NOS). The NOS then compares the hash encrypted password to a stored copy of the hash encrypted password to verify or authenticate the user. [4]

Hashing is not reversible and hence should not be used as a method to encrypt data for subsequent decryption and data retrieval. Hashing algorithms also do not require a key; therefore key length is not an issue or consideration. [5]

As I have previously stated encryption can function actively at the application level, the network level, and at the host level of data transmission and information flow. Therefore, the uses of encryption that I will briefly discuss are the following: E-mail Encryption (giving especial attention to the use of Identity Based Encryption in this area); Encryption in Network Security; Database Encryption; Encrypted Audit Logs; and Tape Encryption.

Security in e-mail transmission can be enabled by encryption which provides senders and recipients with assurances that their e-mail messages have confidentiality, authenticity, and non-repudiation (prevention of a sender from refuting what was sent within an e-mail message).

Currently the encryption standard for major e-mail vendors such as Microsoft, Netscape, Lotus, and Novell is provided by S/MIME which is an encryption technology that uses asymmetric encryption and the X.509 Certificate (also called a Digital Certificate or Digital ID). In S/MIME applications, the public key is placed into a Digital Certificate at the creation of the key pair. The Digital Certificate also contains specific information about the user who owns the public key and therefore confidentiality, authentication, and non-repudiation is provided in a secure e-mail technology. [15]

Identity Based Encryption (IBE) is a public key encryption system which is used in encrypted e-mail and in which an arbitrary string can be used as the public key. IBE was first formulated by Adi Shamir in 1984; however, the first usable scheme for IBE was brought forth in 2001 by Boneh and Franklin [9]. IBE is utilized by major healthcare and financial institutions as well as by the U.S. Government. IBE uses well known identifiers (or an arbitrary string) such as an e-mail address as the public key in a public key/private key pair. IBE utilizes a key server and

allows security policies and authentication procedures to be directly encoded into the encryption process and therefore enables data protection without the use of certificates and Certification Authorities. [17]

To illustrate how IBE works, consider the following example:
Jane (jane@a.com) wants to send a secure e-mail to Tarzan (tarzan@b.com).
Four operations must occur:

1. Setup: An encryption key server inside Jane's firm is initialized with two pieces of mathematically-linked data: a "master secret" and a "public parameters". The master is kept secret by the key server, while the public parameters are distributed to all users in the system. This occurs once.

2. Encryption: To encrypt her message to Tarzan, all Jane requires is Tarzan's e-mail address which is entered and combined with the public parameters by the key server to generate a public key that is used to encrypt the message.

3. Extraction: Tarzan needs a private key to obtain Jane's encrypted e-mail. In an IBE system the private key is generated by the key server. Therefore, Tarzan must request a private key from the key server. When this request is entered the key server mathematically combines the "master secret" and Tarzan's e-mail address to generate Tarzan's private key, which is then sent to him.

4. Decryption: Tarzan uses his private key to decrypt the encrypted e-mail (End of Story). [18]

Besides allowing Jane (or any user) to encrypt an e-mail to anyone who has a valid e-mail address, IBE eliminates the need for certificates or Certification Authorities. IBE also has been incorporated into various security modules that enable encryption to be triggered by one or several combinations of structured data matches (credit card numbers, social security numbers, HIPPAA codes, ABA routing numbers, etc.), unstructured data matches (the presence of confidential information as detected by the respective security module), keywords and regular expressions, and message origin or destination (a specific business partner or supplier). [16]

One disadvantage of the IBE system is that a private key generator (key server) is responsible for generating private keys for all users and this can present a performance impediment for entities with a large number of users. One proposed solution to this potential problem, however, can be found in the construction and use of a forward – secure hierarchical identity –based encryption scheme (fs-HIBE) that allows each user in the hierarchy to refresh his or her private key periodically while keeping the same public key.[9]

In terms of network security and encryption, I will comment briefly on the following: SSL and S-HTTP.

Secure Socket Layer (SSL) is an Internet-standard network encryption and authentication protocol that originated by Netscape. SSL uses encryption to ensure data confidentiality and integrity and these uses are relatively transparent to the end user or application. Many browsers

support SSL and end users don't have to do anything special to enable SSL encryption. SSL encryption occurs at two levels: Low-Level SSL and High-Level SSL. Low-Level SSL encryption is encryption at 40- or 56- bits. High-Level SSL encryption is encryption at 128- bits and is the strongest form of SSL encryption. SSL can provide privacy and a secure connection between a client and a server, however, SSL is much slower than the traditional unsecured TCP/IP connection and this is a direct result of providing security. The initial handshake between the server and the client (which is required for them to authenticate each other and agree on a key, involves a large use of public key cryptography) is a very slow process. To mitigate this effect and to speed up SSL, hardware acceleration has been used. Lastly, SSL can protect data in transit; however, it has no capabilities for protecting data before it is sent or after it arrives at its destination. [20]

Secure-HTTP (S-HTTP) can be used in conjunction with SSL and it can provide security for individual messages. In contrast to SSL which can only authenticate a server, in S-HTTP, a client can issue a certificate to authenticate a user. [20]

The Internet Engineering Task Force (IETF) has approved both SSL and S-HTTP as standards. [20]

With regard to database encryption, encryption can be performed either within the database or outside the database.

If the DBMS supports the encryption of data within the database, data can be transparently encrypted and decrypted within the database as soon as it is stored in the database. However, as data enters or leaves the database it is transported as clear text, which may present performance penalties and security concerns. [22, 24]

Another concern that arises when data is encrypted within the database is that some vendor supported encryption may provide either all or nothing encryption capabilities – either the entire database is encrypted or no encryption occurs. This may lead to database performance degradation because the DBMS is called upon to perform additional processing on data that is not required. Additionally, if the encryption keys are stored in the database they will be accessible to anyone who may have access to the database.

Overall, encryption within the database provides encryption and decryption within the database and leaves the stored legacy applications and other applications unaffected, but it does not provide secure key management or high database performance. [22, 24]

A more secure database encryption protocol is the implementation of encryption outside the database. Since the data is encrypted within the application that introduces the data into the system, the data not only travels encrypted but it can be stored in encrypted form upon its arrival at its destination in the database, which provides end-to-end data protection. [22, 24]

To obviate any modifications to applications to provide support for encryption, an Encryption Server can be purchased and utilized to provide centralized encryption functions for the entire database. The encryption keys are not stored in the database but in hardware (The Encryption

Server) which is separated from the encrypted text. The Encryption Server adds still another layer of protection because the keys in the Encryption Server have to be found before a hacker can decrypt any data. [22, 24]

To be optimally effective, this protocol requires that the Encryption Server be harden against intrusion by the implementation of a strong authentication and control strategy which permits only authorized users to have access to the Server, which provides continuous monitoring of it for suspicious activity, and which provides for the maintenance and regular auditing of an event log. [22, 24]

Some methods of authentication to control access to encryption keys include the following: Password –Based Encryption; Smart Cards; and Biometrics.

Password-Based Encryption (PBE) utilizes hashed encryption keys based on PBE standards and to unlock an encryption the end- user must know the password. The disadvantage to this approach is that it is only as strong as the password. Another disadvantage to this approach is that if too many passwords are used, the system may become too complex to use properly. [1]

Smart cards or Cryptography Tokens offer stronger two-factor authentication (as opposed to single –factor password – based authentication) because smart cards are based on what the user has (the smart card) and what the user knows (a secret PIN or password). Smart cards are easy and simple to use and can be used in situations that require multiple passwords. Additionally, smart cards allow the implementation of audit trails to ascertain what individual accessed what data and when that individual accessed the data. [1]

Biometrics is another method of providing authentication to control access to encryption keys. Biometrics is based on a unique physical characteristic or attribute of an individual (e.g. a fingerprint, voice or retinal scan). When used in combination with password and/or smart cards, biometrics provide very good authentication for controlling access to encryption keys. [1]

Audit logs are a significant part of any secure IT system and they may contain sensitive information that should be protected from the scrutiny of unauthorized parties. B.Waters of the Computer Science Dept. at Princeton University, and D.Balanz, G. Durfee, and D.Smetters of the Palo Alto Research Center have formulated and implemented a searchable (using SQL queries)and encrypted (using hash chains and Identity Based Encryption) audit log that provides tamper resistance, verifiability, and data access control. [23]

Lastly, I will briefly comment on tape encryption. Tape encryption is needed because the storage of data on tape creates breaches and risks in data security from several aspects.

Tapes are often taken off-site to a data vault and this is frequently accomplished by the lowest cost method, that is, by the lowest cost courier company. Further, data saved to tape may not be given any security access levels, and, therefore, an operator can initiate an unauthorized copy of the tape (and there is no way to tell if a tape has been copied). [1, 20]

Therefore in view of the aforementioned, tape encryption may be needed ,but it also may be a requirement for certain institutions such as banks (GLBA ,SEC) and insurance companies, and it may prove to be very useful to Medical Companies (HIPAA) and Research Groups (where data may be indispensable and priceless).[1,20]

THESIS

Encryption is one of the most effective means available to achieve optimal IT control and to assure the integrity and verifiability of data and information, yet it is often not fully understood in terms of its usefulness, not fully appreciated or utilized in terms of its cost-benefits and effectiveness, and often not distinguished from moderately effective access control.

RESEARCH METHODOLOGY

The research methodology in this paper consists solely of personal interviews of selected key IT individuals and personnel.

RESEARCH FINDINGS

Mr. Phillip Cotton, LAN Director, UAB School of Business:
Interviewer: "What encryption, if any, do you use?"
Interviewee: "I only use encryption for log-in, password purposes."
Interviewer: "Why?"
Interviewee: "There is no sensitive data here; I could envision its use, but there is a cost…um…I feel that the faculty would feel that their functions would be impeded."

Mr. Gregory Myers, LAN Director, UAB School of Engineering:
Interviewer: "What encryption, if any, do you use?
Interviewee:" We don't use it."
Interviewer: "Why?"
Interviewee: "I don't see that there is a need for it."

Ms. Susie Corbett, IT section, Lister-Hill Library, UAB:
Interviewer: "What encryption do you use?"
Interviewee: "We don't use it."
Interviewer: "Why?"
Interviewee: "There is no need for it."

Jason Bradley, AM-South Bank, Manager, Internet Banking:
Interviewer: "What encryption does your bank use?"
Interviewee: "We use it, but I can't discuss it!"

"Jack", Medical Records Supervisor, Health South Medical Center:
Interviewer: "What encryption do you use?"
Interviewee: "We don't use it."
Interviewer: "Why?"
Interviewee: "There is no need."

Ms. Jill Gemmill, Assistant Director of Academic Computing, UAB:
Interviewer: "What encryption do you use?
Interviewee: "We use SSL to provide secure communications to our servers; we use 20-48 bit block ciphers."
Interviewer: "Do you use both symmetric and asymmetric key encryption?"
Interviewee: "Both."
Interviewer: "Do you use crypto-capable routers?"
Interviewee: "No."
Interviewer: "Do you use one-way (hash) encryption?"
Interviewee: "Yes."
Interviewer: "Is there an exchange of certificate requirement to send an encrypted message in your system?"
Interviewee: "Yes."
Interviewer: "Do you see any problem with this handshake requirement?"
Interviewee: "No."
Interviewer: "Do you use Identity Based Encryption?"
Interviewee: "No, but I can see a need for IBE. I would like to see e-mail encrypted, however, cost is a factor… not a financial cost factor… I mean in terms of cost of training, set-up, and infra-structural requirements."
Interviewer: "Do you use tape encryption?"
Interviewee: "No."
Interviewer: "Do you view encryption as an effective means of IT control?"
Interviewee: "The default level of security in a university environment is open. We like to have a good balance between openness and security. We have 20,000 computers and servers at UAB and at least once a week we experience an intrusion primarily from the Internet… from places like Estonia and Latvia and not necessarily from UAB students or other students."

Mr. Mike Whitt, Director of Information Security, Compass Bank.
Interviewer: "What encryption do you use?"
Interviewee: "We only use standardized encryption."
Interviewer: "Where is your encryption used most frequently?"
Interviewee: "Our biggest use of encryption is in our data transmission over the internet."
Interviewer: "How many bits are used in your encryption?"
Interviewee: "We use 128 bit encryption… and some 256 bit encryption, sparsely."
Interviewer: "What has been your experience with encryption – good or bad?
Interviewee: "Good. No problems, cost is the main issue."
Interviewer: "Do you use symmetric or asymmetric key encryption and do you use crypto-capable routers?"
Interviewee: "Yes to all!"
Interviewer: "Do you use one-way (hash) encryption?"
Interviewee: "In certain situations – passwords, etc."
Interviewer: "Do you use encryptions in Virtual Private Networks and in the LAN context?"
Interviewee: "Yes to both."

Interviewer: "Is there any handshake or exchange of certificate requirement to send and encrypted message outbound?"
Interviewee: "Yes."
Interviewer: "Do you see any problems or disadvantages with your forms of encryption?"
Interviewee: "No problems."
Interviewer: "Do you use Identity-Based Encryptions (IBE)?"
Interviewee: "Compass does not use IBE, however, I think that it is an excellent concept, but I feel that it would be hard to justify the cost."
Interviewer: "Do you use tape encryption?"
Interviewee: "No, but in the near future we will, because we are mandated by SEC to use it within a year."
Interviewer: "Do you view encryption as one effective means of IT control and security?"
Interviewee: "The use of encryption is an excellent control mechanism; however, cost is of primary concern."

ANALYSIS OF FINDINGS

The interview findings seem to support this writer's thesis that encryption is an effective means of IT control and security implementation and that its usefulness is not well appreciated or put to optimal use (at least in the local area). Clearly, in the School of Engineering, encryption would be useful in the form of an encrypted (IBE based) e-mail capability and in the encrypted storage of data and information because in that entity a large amount of research is being generated, some of which may be sensitive, classified and/or designated for patent rights.

Although classified research may not be undergoing in the School of Business encrypted (IBE based) e-mail would be useful in that entity as well.

In terms of cost benefit analysis, clearly the benefits of having secure, protected information, and the preservation of confidentiality and privacy of e-mail would outweigh the nominal cost of IBE.

The interview findings also support the thesis supposition that the distinction between access control and encryption is often blurred. This is supported by the interview findings with Mr. Cotton, Mr. Myers, Ms. Susan Corbett, and the Supervisor of Medical Records ("Jack") at Health South Medical Center. As I have discussed, Identity -Based Encryption is compatible with security modules that allow effective and efficient transmission of information that has structured data matches and unstructured data matches, that would not impede accessibility to data and information, and that would also concurrently provide for authentication, confidentiality, and non-repudiation.

That UAB still uses Low-Level SSL encryption (revealed in the interview with Ms. Gemmill) comes as a surprise. As I have discussed in this paper the minimal effective block cipher encryption should be 128-bit length.

That encryption is an effective means of IT control and security is supported by the interview with Mr. Mike Whitt, Director of Information Security at Compass Bank. Therefore, while

encryption is not a control or security cure-all, it is a very important tool in addressing specific risks and threats.

CONCLUSION

Identity theft and invasion of privacy are increasing even as the risks of data disclosure are on the rise. Increasingly, health care, financial, and other institutions must deal with legislation and regulations on data privacy, and in view of current news reports regarding cyber-terrorism, consumer concerns about data disclosure and misuse will probably expand the responsibilities of most enterprises and institutions to secure customer information. In this environment, therefore, an IT control and security plan must include a strategy for protecting sensitive data and information against attack or misuse by implementing an effective encryption protocol.

REFERENCES

[1] Securing Data at Rest: Developing a Database Encryption Strategy, RSA Security Incorporated, www.rsasecurity.com

[2] How to Offer the Strongest SSL Encryption, VeriSign, White Paper, www.verisign.com/products/site

[3] Polar Crypto Component; Technical FAQ, http://www.polarsoftware.com/products/crypto/techfaq.asp

[4] Essentials of Networking: Enterprise Network Security-Encryption and Firewalls, http://home.att.net/~s.k.vincent/net121_18.htm

[5] Cryptographic hash function, http://en.wikipedia.org/wiki/cryptographic_hash_function

[6] http://cisr.nps.navy.mil/guests/martin04.html

[7] IBE Applied to Privacy and Identity Management. http://www.netcorp.org/IBE.html

[8] Identity-Based Encryption, http://www.cap-loore.com/crypto/ibe.html

[9] ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption, D.Yao, N.Fazio, Y. Dodis, and A. Lysyanskaya. Cryptology ePrint archive, Report 2004/212, 2004.

[10] Minimal-Overhead IP Security using Identity based encryption G. Appenzeller and B. Lynn, appenz@c.s.standford.edu

[11] IBE Secure E-mail, http://crypto.stanford.edu/ibe/

[12] Returning Privacy to E-mail, http://www.templetons.con/brad/crypt.html

[13] Identity-Based Encryption, http://www.noretech.com/

[14] Domain-Based Administration of Identity Based Cryptosystems for Secure E-mail and IPSEC, D.K. Smetters and G. Durfee, http://www.usenix.org/event/sec03/tech/full_papers/smetters/smetters_html/

[15] E-mail Encryption, http://www.idexsys.com/smime.htm

[16] http://www.chi-publising.com/index.php?newsIDE=361

[17] The New Solution: Identity -Based Encryption, http://www.securenetcom.com/technology.htm

[18] http://www.massagingpipeline.com/60404975

[19] Introduction to Network Security, M. Curtin, http://www.interhack.net/pubs/network-security

[20] Network Security, Goldman and Rawles, http://www.people.memphis.edu/~dwnickls/3790ch13.htm

[21] Automatic Whole Database Encryption-How It works, http://www.netlib.com/how-it-works.shtml.

[22] Database Encryption, http://www.iwar.org.uk/courses/comsec/resources/standards/germany/itpm/s/s4072.htm

[23] Building an Encrypted and Searchable Audit Log, B. R. Waters, D. Balfanz, G. Durfee, D.K. Smetters, bwaters@cs.princeton.edu

[24] A Conceptual Overview of Public Key Encryption. J.G. DeRose, http://jasonderose.org/sopke.html

[25] A Database Encryption Solution, Ulf.T.Mattsson, http://www.linuxsecurity.com/content/view/116068/65/